Mumbai University

May – 2018

B.Sc.IT: Semester – V

(Question Paper)

[IDOL – Revised Course]

Paper – I

Network Security

Time: 3 Hours **Total Marks:** 100

N.B.: **(1)** *All Question are Compulsory.*
(2) *Make Suitable Assumptions Wherever Necessary And State The Assumptions Made.*
(3) *Answer To The Same Question Must Be Written Together.*
(4) *Number To The Right Indicates Marks.*
(5) *Draw Neat Labeled Diagrams Wherever Necessary.*
(6) *Use of Non – Programmable Calculator is allowed.*

Q.1 ATTEMPT ANY TWO QUESTIONS: (10 MARKS)

(A) Describe OSI Security Architecture. **(5)**
(B) What is Signature Scheme? List some of its examples. **(5)**
(C) What are the groups of IP Security Document? **(5)**
(D) Write a note on IKE (Internet Key Exchange) Protocol & SA (Security Association). **(5)**

Q.2 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) What are the different modes of DES? Explain any one in detail **(5)**
(B) What are Ciphers? What is the difference between "*Transposition Cipher*" and "*Substitution Cipher*"? **(5)**
(C) Explain the working of DES. **(5)**
(D) Explain p-1 Factoring Algorithm. **(5)**
(E) Define Cryptosystem. Explain it with suitable diagram. **(5)**
(F) Explain the working of Affine Cipher with an example. **(5)**

Q.3 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) Write a short note on ElGamal Signature Scheme. **(5)**
(B) What is the concept of Birthday Attack? Explain. **(5)**
(C) Explain Digital Signature Standard. **(5)**
(D) What is Signature Scheme? List some of its examples. **(5)**
(E) What are the types of different Attack Models of Signature Scheme? **(5)**
(F) Describe Diffie-Hellman Key Exchange Algorithm. **(5)**

Q.4 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) What is active attack? Illustrate your explanations. **(5)**
(B) Define Computer security and objectives of computer security. **(5)**
(C) Explain Network security model in detail **(5)**
(D) Explain the different types of attacks. **(5)**
(E) Explain the following terms: **(5)**
(i) *Authentication*
(ii) *Access Control*
(iii) *Non-Repudiation*
(F) Explain "*Replay Attack and Traffic Analysis*" with suitable examples. **(5)**

Q.5 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) What is Public Key Infrastructure? What are the required functionalities for that? **(5)**
(B) Describe S/MIME with a neat diagram. **(5)**
(C) Explain the working of Pretty Good Privacy. **(5)**
(D) What are the various Web Security Protocols? **(5)**
(E) Explain PKCS System. **(5)**
(F) What four requirements were defined for Kerberos? **(5)**

TURN OVER

Q.6 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) Give examples of situations where IPSec is used? **(5)**

(B) Explain the various participants in SET (Secure Electronic Transaction). **(5)**

(C) What are the Services provided by IPSec? **(5)**

(D) What is the difference between SSL Connection and SSL Session? **(5)**

(E) What are the Business requirements for Secure Payment processing with Credit Cards over the Internet? **(5)**

(F) What is the difference between Tunnel Mode and Transport Mode with respect to IPSec? Why does ESP include a Padding Field? **(5)**

Q.7 ATTEMPT ANY THREE QUESTIONS: (15 MARKS)

(A) What is Intrusion Detection System? Explain its benefits. **(5)**

(B) List and explain Four Techniques used to avoid Guessable Passwords. **(5)**

(C) Explain the Different Firewall Configurations. **(5)**

(D) Explain briefly the Classes of Intruders. **(5)**

(E) Write a short note on DDoS. **(5)**

(F) What is a Firewall? List its advantages and disadvantages. **(5)**
